Copy sent H.C.S.G.
W/Cdr Badcock.
Section V.
3/10.

15 (GT)

TOP SECRET

TICOM/I-121

TRANSLATION OF HOMEWORK BY OBLTN. W.WERTHER, COMPANY COMMANDER OF 7/LN. RGT. 353, WRITTEN ON 12TH AUGUST, 1945 AT A.D.I.(K)

The attached report covers:-

a. P/W's career.
b. Various cypher systems handled by G.A.F. cryptanalysts.
c. Organisation of Chi-Stelle East
d. The Forschungsamt.

TICOM

No. of pages: 12

27th Sept. 1945.

DISTRIBUTION

British

D.D.3
H.C.G.
D.D. (N.S.)
D.D. (M.W.)
D.D. (A.S.)
C.C.R.
Lt. Col. Leąthem
Cdr. Tandy
Major Morgan

U.S.

Op-20-G (2) (via Lt. Cdr. Manson)
G-2 (via Lt. Col. Hilles)
A.S.A. (3) (via Major Seaman)
Director, S.I.D. USFET
(via Lt. Col. Johnson)
Col. Lewis Powell, USSTAF.

TICOM

Chairman
S.A.C. (3)
Cdr. Bacon
Lt. Col. Johnson
Major Seaman
Lt. Cdr. Manson
Major Cowan
Lt. Fehl
Ticom Files (4)

ADDITIONAL

Lt. Col. Thompson
S.A.C. for Signals 5, Air Ministry.
S.A.C. for Section V
(Item XIV)

12. 8. 45.

Waldemar WERTHER

Oberleutnant and O.C. Coy.
7/GAF Signals Regt. 353

C A R E E R

Born 2.6.1913 at ODESSA in SOUTH RUSSIA. Son of Viktor WERTHER, manager of a commercial undertaking, and his wife Helen, daughter of Leonard KOSITZKI-KORSUCHIN of IRKUTSK in SIBERIA, owner of a gold mine.

Beginning of 1919, flight from the Bolsheviks into SWITZERLAND via SOUTHERN EUROPE.
1920-25, resided in GERMANY (ERFURT and BERLIN) and attended school there.
1925-31, resided in RIGA (LATVIA) where attended school
June 1931 passing-out examination at the German High School for Natural Sciences in RIGA.
1931-36, frequently interrupted and unfinished study of political science at BERLIN University and at the AUSLAND-HOCHSCHULE in BERLIN. Employed simultaneoulsy as Works student, especially in scientific and journalistic work with agricultural press and propaganda offices, at exhibitions and in broadcasting. Several journeys (FINLAND, ESTHONIA, LATVIA, AUSTRIA, SWITZERLAND, FRANCE).

In the spring of 1933 my Students' Corporation volunteered in a body for the S.A., to which I belonged until I entered Voluntary Labour Service in January '34. I stayed voluntarily in the Labour Service for 14 months. - I joined the National-Socialist Party in May 1938 at the request of my department.

In June 1939 I married Hetty RAPPE, a Red Cross Sister, daughter of Carl RAPPE, a landowner of KORBACH/WALDECK. I am the father of two children aged $5\frac{1}{2}$ and $2\frac{1}{2}$ years. - My family is at KORBACH/WALDECK (U.S. Zone). My parents are probably in POTSDAM; I have no news of them since January '45.

Technical Career.		Military Career.
Entered the service of the GAF	1.1.37	
Interpreters examination in RUSSIAN at the AUSLAND-HOCHSCHULE in BERLIN	Jan.37	
Civilian wireless training with GAF Signals ABTEILUNG at BERNAU near BERLIN	Jan.-Mar.37	
	Mar.-Jly.37	Basic training as wireless operator with GAF Signals Training Company in BERLIN-KLADOW; promotion to GEFREITER (Reserve), recommended as Candidate for a Commission in the Reserve

Technical Career	Military Career
Practical training as cryptographer in the Listening Service Section of the German Air Ministry (later CHI-STELLE). Employed as cryptographer, chiefly against the SOVIET UNION	Jly. 37.- Dec. 38.
Director of cryptography with W.z.b.V. in BUDAPEST	Jan.-June 39
Deputy Director of Section E1, (Eastern Cryptography) of the CHI-STELLE. Current work on all systems encountered, technical advice service for out-stations and training of cryptographic personnel. War service in POTSDAM, EAST PRUSSIA and UKRAINE.)	June 39 - Aug. 42.
	April 40 Posted to 14/GAF Signals Regiment Ob. d. L. (CHI-STELLE) while retaining technical funotion and responsibilities.
	1.8.40 Promoted to Uffz. (Reserve)
	Dec. 40 Awarded War Service Cross 2nd class with swords.
	1.1.41 Promoted Feldwebel (Reserve)
	1.4.41 Promoted Leutnant (War Substantive)
	Dec.41 (Awarded War Service Cross 1st class (with swords
Director of Cryptography in the northern sector of the Eastern Front (Luftflotte 1))	Aug.42 - Aug.43 Officer of the Watch with 14/GAF Signals Regiment 1 (later 1/GAF Signals Regiment 353)
	1.7.43 Promoted Oberleutnant(War Substantive)
Director of Cryptography in the central sector of the Eastern Front(Luftflotte 6))	Sept. 43 - 8.5.45
	Sept. 43 - May 44 (Officer of the Watch with 10/GAF Signals Regiment 35 (Later 7 (GAF Signals Regiment 353)
	March-April 44 Course for Acting O's.C.Coy. in NANCY.
	May 44 Acting O.C. Coy. 7/353
	July 44 Promoted O.C. Coy. 7/333

(signed) W. WERTHER

SOME PARTICULARS OF CIPHER SYSTEMS ON WHICH WORK WAS DONE BY GAF CRYPTOGRAPHERS

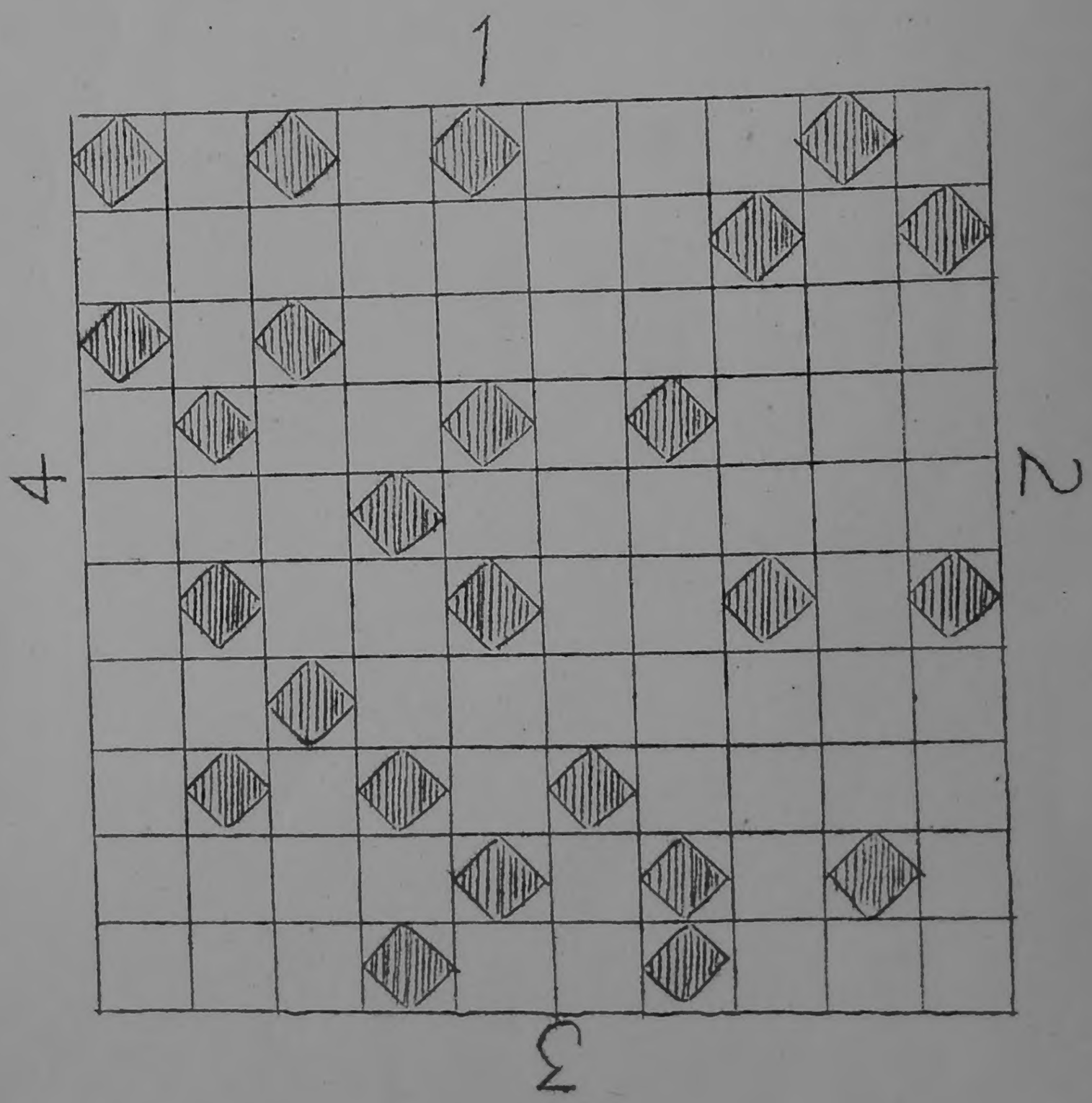
I. LITHUANIA.

Section E1 of CHI-STELLE began to monitor the wireless stations of the LITHUANIAN Air Force at the beginning of 1938. Although no cryptographers with a knowledge of the language have been available, success in breaking the cipher of the ground organization was achieved in a very short time. From then onwards until the Red Army entered LITHUANIA late in the summer of 1939, the messages were read currently by the out-station at INSTERBURG, which later transferred to KOBBELBUDE. Change of cipher instructions delayed breaking by as much as 1 to 2 days.

The basis of the cipher

A 10 x 10 grid with 25 cut-out squares. The sides of the grid were numbered 1 - 4.

Reconstruction of a grid:



The grids were changed at irregular intervals.

Enciphering.

The clear text is written from left to right and from top to bottom in a 10 x 10 square of a size to fit the grid. The number of text elements must be divisible by 10; any squares remaining free on the last line of the text are filled up by a partial repetition of the signature.

Example: a n h p t (.) v i t a *
u t i s (.) a n k o m
m e a m 7 (.) 1 2 (.) 3
8 z u r b e s i c h
t i g u n g d e s f
l u g p l a t z e s
(.) o b e r s t t o m
a l u n a s t o m a

On the other hand the signature could, if necessary, be abbreviated, but this occasionally led to queries by the receiving station.

Example

a	n /	h	p	t	(.) /	v	i	t	a
u	t	i	s	(.) /	a	n	k	o	m
m	e /	a	m /	1	6	(.)	1	1	(.)
3	8 /	u	m /	1	0	u	h	r /	z
u	r /	b	e	s	i	c	h	t	i
g	u	n	g /	d	e	s /	f	l	u
g	p	l	a	t	z	e	s	(.) /	o
b	e	r	s	t /	t	o	m	a	l
							(u	n a s)	

**

Translator's Notes * The supposed LITHUANIAN text is given in German and reads: "To Hpt. VITAUTIS. I arrive on 7.12.38 to inspect the airfield. Oberst TOMALUNASTOMA"

** Translation of German: "To Hpt. VITAUTIS. I arrive on 16.11.38 at 1000 hours to inspect the airfield. Oberst TOMAL."

The grid is superimposed four times on the square into which the clear text has been written. The sequence in which the four operations are carried out is dictated by the reciphering group for the day: this is expressed by four figures - made up of the figures 1 - 4, corresponding to the sides of the grid. This group does not, however, appear as indicator in the cipher text. The symbols appearing in the cut-out squares of the grid are written out, again from left to right and from top to bottom, and made up into groups of ten.

Example: Grid (see page 4)
Clear text (see example on page 5)
Reciphering group for the day: 1 3 4 2

(1) a h t t k m m a 8 1 u e u d f u l e s t

(3) p v t s a 1 . 1 h u b i t s a z . m l

(4) i a i . n m 1 . 3 u 0 r s c i n g p e t a

(2) n . u o e 6 m r z h g g e l t s o b r o

Cipher text.- ahttkmma81 ueudfulest pvtsa1.1hu
bitsaz.mli ai.nm1.3u0 rscingpeta
n.uoe6mrzh ggeltsobro +

Deciphering

The cipher text is deciphered by carrying out the same processes in reverse order.

Criticism of the System.

The security of the cipher is low. The figure groups in the cipher text are particularly vulnerable, since they can often be combined without difficulty to form a date group or a time.

As a general rule it was also possible to recover the original designations of the grid sides, because in case of difficulty in deciphering the station at the other end was inter alia in the habit of transmitting the original key group (the indicator).

II. POLAND

Work on POLISH material was begun only a few weeks prior to the POLISH campaign with a very small and inadequate staff: hence it did not yield any concrete results. Reading POLISH take-off and landing reports was the only success achieved.

A captured code-book seen by the author contained some 2000 significations; it was - as far as I can remember - hatted and reciphered approximately as follows:

Reciphering of Code-book pages: unknown.

Reciphering within the individual pages (quadrant and line) see example.

Example: CAPTURED POLISH CODE-BOOK

Code-book open at page with quadrant and line reciphering placed alongside.

0 2 8 8 9 6 3	Pos. 1				1 8 6 7 5 0 3
7 1 3 0 0 4 6			Pos. 2	Pos. 4	1 2 7 4 5 6 9
4 3 9 2 2 1 7		Pos. 3			3 2 8 6 5 4 0
8 9 7 5 5 3 4					7 5 8 3 6 1 9
7 1 0 1 8 2 5					2 8 3 9 6 4 0

Every page of the code-book is divided into a left half and a right half. The left-hand row of reciphering figures (black) are valid for the left halves of the pages, the right-hand figures for the right halves:

Reicphering of position 1 - .. 88
" " " 2 - .. 47
" " " 3 - .. 22
" " " 4 - .. 49

The separate yellow-bordered rectangles in the example were galalith plates(with symbols on both sides?) which could be conveniently exchanged and transposed to vary the reciphering.

III. CZECHOSLOVAKIA

Reg. Rat VOEGELE began to work on CZECHOSLOVAK (five-letter) air messages at an early stage (beginning of 1937?), but no concrete results were achieved.

Part of the material was recognised as being practice traffic without tactical significance, it was also possible to reconstruct practice tables from which, on the basis of indicators, the message groups could be read according to predetermined rules. The station at the other end could check the messages received by using the same table and thus trace receiving or transmitting errors on the part of the operators.

Of the tactical material, only a few transposition messages were read.

According to Reg. Rat VOEGELE, the remaining material was machine cipher.

IV CARPATHO-UKRAINE

Messages (5-letter) were read at W.z.b.V. in BUDAPEST which were on a systematic substitution.

Example:

Clear ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher ← ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ →

The cipher text slide was movable. Every message was differently enciphered. The security of the cipher was nil.

"Kolonne sofort in Marsch setzen"* would, according to the above setting of the enciphering table, be:
waxaz z ear adfuz ymdeo tegfl qz+

V. RUMANIA

1. The Air Force Cipher.

In the spring of 1939 the writer was, in the course of his duties with W.z.b.V. in BUDAPEST, posted at the request of the Hungarians to the Hungarian Foreign Office to work on the Rumanian Air Force Cipher. Since the writer does not know Rumanian, he was given an interpreter without technical knowledge to advise him on linguistic matters and to assist him generally.

Analysis yielded very pronounced characteristics; it was a transposition system. As far as I can recollect, the number of letters in all (five-letter) cipher messages could always be reduced to the square of even numbers, thus:

6 x 6 = 36 + 4 dummies = 40 letters
8 x 8 = 64 + 1 dummy = 65 letters
10 x 10 = 100 + 0 dummies = 100 letters
12 x 12 = 144 + 1 dummy = 145 letters
14 x 14 = 196 + 4 dummies = 200 letters etc.

A few days after the well-founded report that a break into the cipher was to be expected in a very short time, the author was transferred back to the Chi-Stelle and the work was carried on (as a matter of form ?) by unqualified cryptographers. In the circumstances it was natural to assume a deliberate interference with the work (for political reasons?). As far as is known the system was not solved but later bought by the Hungarians.

Trns: * "Send off the column immediately."

2. The Police Cipher.

The Police cipher was read currently but I can no longer recollect details. It was, however, so elementary that suggestions were put forward to the effect that the Rumanians be induced to alter this cipher, since for example exact information was being transmitted on the police network about the German troops moving into the country and it was to be assumed that the Allies were monitoring this traffic intensively. It may even be assumed that this was a case of camouflaged treason on the part of the Rumanian authorities.

IV. YUGOSLAVIA

Work was started in such good time that at the start of the Yugoslav campaign there were available very well prepared cipher data and the listening service was able to give continuous and admittedly important information on the enemy. The delay in reporting was negligible.

Cipher data

Lexicographic table with about 30 columns and about 60 lines.

Reciphering

Columns (AB) and Lines (CD) were reciphered, originally with non-hatted and later with hatted rows (or substitution tables)
As far as I can remember, indicators gave the initial values of both the reciphering rows. A change of recipherer was very rarely made.

Criticism of the System

The cipher security of the system was low. No great difficulties were experienced in reconstructing the table, since owing to the non-hatted reciphering rows used in the beginning, all recipherings could be conveniently reduced to one another and in addition, the original build-up was not concealed by thr recipherings.

VII. TURKEY and

VIII. GREECE.

The Air Force ciphers were very elementary. Details not known.

IX. FRANCE

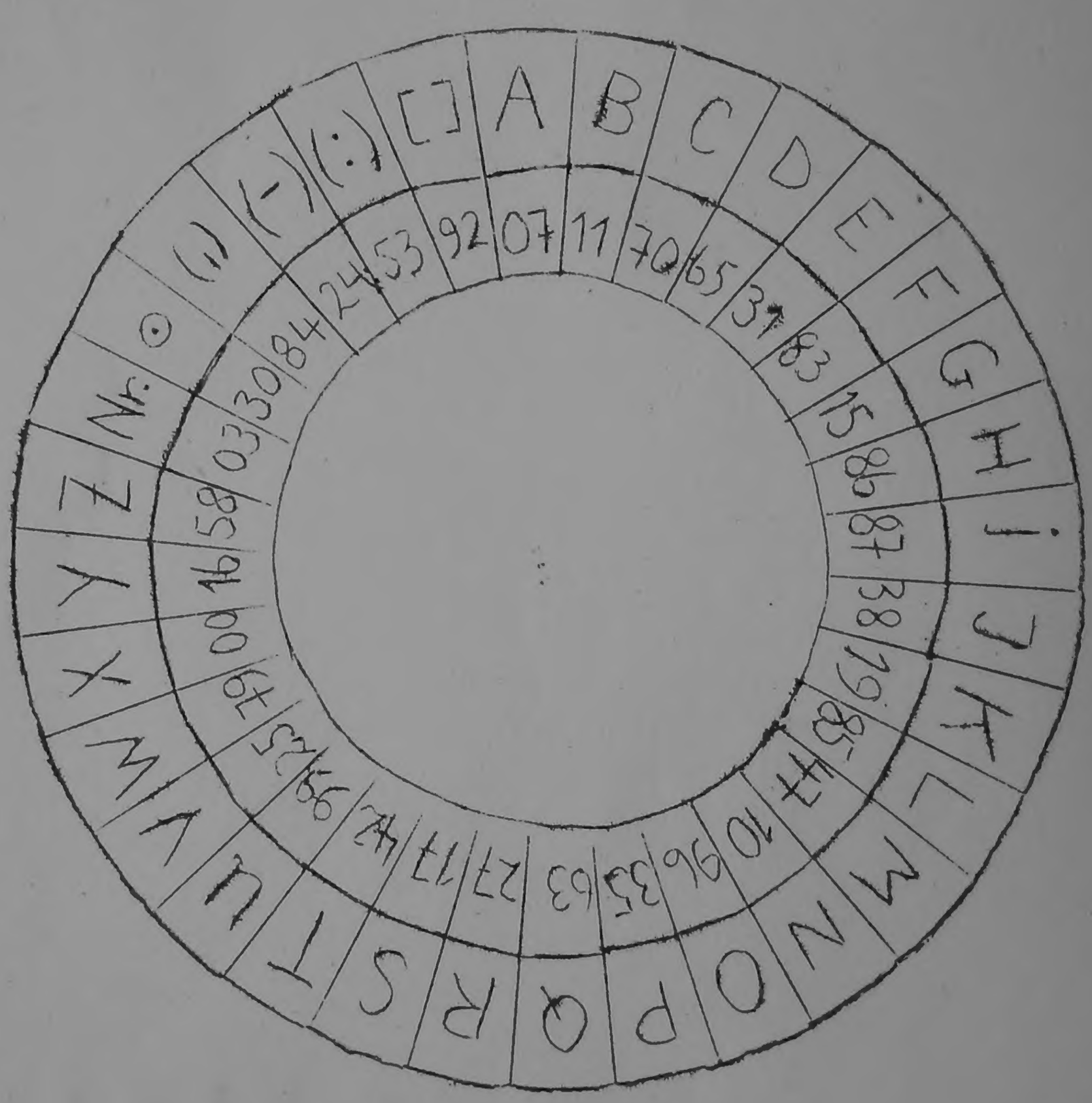
As far as I can remember, a basic book was reciphered with short periodic subtractors. Yet these messages could not be broken until a few days before or even after the capitulation of FRANCE.

Nothing known about DE GAULLE methods.

X. SPAIN

During the Civil War, the REDS - as far as is known - transmitted almost exclusively messages in clear.

A reconstructed substitution disc looks roughly as follows:



The smaller (red) disc with the reciphering figures was mounted so as to be movable; thus a series of drum (TROMMEL) variations could be set.

Further particulars concerning recipher changes, use of indicators etc., are not known to the author.

XI. GREAT BRITAIN

1. During the first few years of the war, a comprehensive, hatted and non-reciphered form or five-letter code-book was read. This was the Merchant Navy Code.

Apart from this code-book, however, a comprehensive guide to ships and locations and a substitution table were used to encipher messages. Smooth working in the simultaneous use of these three basic principles was made possible by *switch groups in the message. Externally, the cipher grour arrived at by the various methods were not distinguishable.

2. A daily changing column substitution table ("SYKO"?) for the use of reconnaissance aircraft consisted of about 25 substitution alphabets.

The cipher messages were read currently without special difficulty owing to the wealth of material available. Captured tables facilitated the work in so far as they were used again at regular intervals (monthly ?).

3. Work was also currently carried out on a comprehensive four-figure basic book, but with the frequently changing subtractor books it was impossible to keep pace with this. The subtractor starting-points were indicated in the message by four-letter (?) indicators. Not every subtractor group, however, could be used as an initial group, but only the first group in each case of every second or third (?) subtractor line (ZEILE), i.e. every 10th or 15th group.

XII. U.S.A.

No details known.

The author can, for the following reasons, give no more detailed information on the questions set:

1. The author belonged to Section E 1 till 1942. This section was in fact incorrectly called "'Eastern' Cryptography", since - apart from the LITHUANIAN system - it worked only on the SOVIET UNION, and it neither controlled nor watched those working on other EASTERN EUROPEAN countries.

2. The ciphers of the EASTERN and SOUTH-EASTERN EUROPEAN countries

*Trns: German "SIGNAL"

were nearly all elementary ciphers which were mostly dealt with independently by the corresponding out-stations. Only Yugoslavia was dealt with at Marstall also.

3. The systems of the Western Powers were indeed also originally worked on at Marstall (Section E 2, Reg. Rat VOEGELE), but in this case the main effort on the different systems was very soon transferred to the various out-stations. In addition, the visits paid for the purpose of keeping in the general picture to workers engaged on miscellaneous systems were always very short, owing to lack of time, and therefore insufficient to leave one's memory with permanent impressions.

[initialled] W.

XIII. ORGANIZATION OF CHI-STELLE EAST

In practice, both Eastern sections of Chi-Stelle (D/evaluation, E1/breaking) were merged in the Regimental Evaluating and Breaking Departments; the brains of the Eastern Organization, Major KUPFFER, became Liaison Officer with the G.A.F. Ops. Staff. Only two members of the Chi-Stelle remained with the Regiment, viz. Lt. WISNIKOW (evaluation) and Lt. V. LINGEN (breaking), but their influence on the organization of the work in the east was very small, all the more so as they were rejected by the Regiment as well as by the Abteilung for practical and for personal reasons.

XIV. THE FORSCHUNGSAMT

The author knows no details concerning the work of the FORSCHUNGSAMT, since the activities of this institution were kept very secret. At any rate diplomatic traffic was worked on or at least collected there. Rumour also mentioned economic espionage. The workers were exceptionally well paid, but very discreet: the author had no personal acquaintances in the FORSCHUNGSAMT.

Nor was it know who was the head of this organization: opinion varied between the REICHMARSCHALL and SS (or both). In RIGA in 1942, the author was invited by an SS-Fuehrer of his acquaintance, who had not been initiated by him into the nature of his activities, to join the SS (?) Cryptography. Perhaps he meant the FORSCHUNGSAMT. The head of the crypto-graphic department was said to be a former naval officer.